

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Protecting Against National Security)	WC Docket No. 18-89
Threats to the Communications Supply)	
Chain Through FCC Programs)	

COMMENTS OF COMPETITIVE CARRIERS ASSOCIATION

Competitive Carriers Association (“CCA”)¹ submits these comments in response to the *Public Notice* in the above-captioned proceeding seeking comment on “how Section 4 of the recently enacted Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act) . . . applies to proposals under consideration” in this proceeding.² CCA strongly supported the passage of the Secure Networks Act and encourages the Commission to view the statute as the primary vehicle for addressing the removal and replacement of covered equipment and services. This proceeding presents an opportunity to implement the statute, including through

¹ CCA is the nation’s leading association for competitive wireless providers and stakeholders across the United States. Members range from small, rural carriers serving fewer than 5,000 customers to regional and nationwide providers serving millions of customers, as well as vendors and suppliers that provide products and services throughout the wireless communications ecosystem.

² *Wireline Competition Bureau Seeks Comment on the Applicability of Section 4 of the Secure and Trusted Communications Networks Act of 2019 to the Commission’s Rulemaking on Protecting Against National Security Threats to the Communications Supply Chain*, Public Notice, DA 20-406, WC Docket No. 18-89 (rel. Apr. 13, 2020) (“*Public Notice*”); see Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) (“Secure Networks Act”).

appropriate modifications to the proposals in the *Further Notice of Proposed Rulemaking*.³ The *Public Notice* raises important questions regarding that implementation process, and CCA appreciates the opportunity to provide input on how the Commission can execute Congress's directives in a manner that provides carriers the flexibility they need in this process to ensure that customers remain connected during the transition. Section I of these comments responds to several of the Commission's questions relating specifically to the reimbursement aspect of implementing the Secure Networks Act. Section II responds to the Commission's questions regarding how to implement the statute's requirements regarding removal, replacement, and disposal of covered equipment and services.

I. THE COMMISSION SHOULD IMPLEMENT A REIMBURSEMENT FRAMEWORK THAT REFLECTS THE REALITIES OF THE REPLACEMENT PROCESS

The Commission asks whether it “should modify the reimbursement program proposed in the *Further Notice of Proposed Rulemaking* to implement” the Secure Networks Act's directions for how the Secure and Trusted Communications Networks Reimbursement Program (the “Program”) should operate.⁴ CCA submits that the answer is a clear “yes.” The Secure Networks Act establishes much of the framework for the Program, such as who may receive reimbursements, what eligibility requirements those providers must meet, and for what purposes recipients may use Program funds.⁵ The Commission has an important role to play in Congress's framework, of course: “establish[ing]” the Program, making reimbursements to eligible

³ See *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, Huawei Designation, ZTE Designation, Report and Order, Further Notice of Proposed Rulemaking, and Order*, 34 FCC Rcd. 11,423 (2019) (“*Further Notice of Proposed Rulemaking*” or “*FNPRM*”).

⁴ *Public Notice* at 2.

⁵ See Secure Networks Act § 4(b)-(c).

providers, publishing and updating a list of “covered communications equipment or services,” and more.⁶ But there are important differences between the Commission’s proposals and Congress’s directives. For example, while the Commission proposes to make reimbursement available only to Eligible Telecommunications Carriers (“ETCs”), the Secure Networks Act requires that funding be made available to any provider of “advanced communications service” that meets the requirements of the Program, regardless of ETC status.⁷

The *Public Notice* asks how the Commission should interpret the phrase “providers of advanced communications service” in the Secure Networks Act.⁸ As provided by the Secure Networks Act: A “provider of advanced communications service” is one who “provides advanced communications service to United States customers.”⁹ And “advanced communications service” carries the “meaning given the term ‘advanced telecommunications capability’” in 47 U.S.C. § 1302¹⁰: “high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology,” “without regard to any transmission media or technology.”¹¹ The Commission need not alter or restrict that language in order to implement the

⁶ *Id.* § 4(a).

⁷ Compare FNPRM ¶ 129 with Secure Networks Act § 4(a).

⁸ *Id.* (citing Secure Networks Act § 9(10)).

⁹ Secure Networks Act § 9(10).

¹⁰ *Id.* § 9(1).

¹¹ 47 U.S.C. § 1302(d)(1). Importantly, the Secure Networks Act does *not* refer to the definition of “advanced communications services” in Section 3 of the Communications Act, which is different from the definition of “advanced telecommunications capability” in Section 706 of the Telecommunications Act of 1996. See *id.* § 153(1) (defining advanced communications services as “(A) interconnected VoIP service; (B) non-interconnected VoIP service; (C) electronic messaging service; and (D) interoperable video conferencing service”).

Program, particularly given that the Secure Networks Act’s expansive aim to “provid[e] for the establishment of a reimbursement program for the replacement of communications equipment or services posing” national security risks.¹²

The Commission also asks how it should modify the “reimbursement program application filing and review process” from the *FNPRM* to implement the statute’s requirements.¹³ CCA encourages the Commission to ensure that its application process permits carriers to list cost estimates for all aspects of the removal process, particularly in light of the statute’s requirement that applicants certify when seeking reimbursement that their plan will result in the “permanent removal and replacement” and “disposal of” covered equipment and services.¹⁴ Transitioning from covered equipment and services to new replacements will be a multi-step process involving numerous entities. The process is likely to include, at a minimum:

- drive testing networks to establish baseline coverage
- evaluating existing spectrum and backhaul capabilities
- ordering new equipment in bulk, sufficiently early in the process to account for lead time required by vendors, which may be many months
- erecting new network cores in parallel with existing cores, which may require facilities expansion and other structural alterations
- evaluating existing cells sites for potential modifications, including additional wired backhaul capacity or alternative microwave backhaul links
- if necessary, renting new towers and obtaining new permits

¹² Secure Networks Act.

¹³ *Public Notice* at 2.

¹⁴ Secure Networks Act § 4(d)(4)(A).

- installing new RAN equipment
- optimizing new components, testing the network, coordinating with local PSAPs
- and ultimately, migrating traffic, and decommissioning old equipment.

The Commission should allow providers to submit cost estimates that cover all stages of the process that apply to them, particularly since many of these steps are not entirely within the control of the carrier. A narrow or inflexible lens for reviewing and acting on applications will make the process inefficient and burdensome for both the Commission and the carriers subject to the statute's requirements.

The Commission also asks about the use of “initial disbursement allocations,” including how deadlines for “completing the removal and replacement process” should be structured.¹⁵ Early, initial funding allocations will be extremely important to the success of the Program. Vendors commonly require significant up-front payments for equipment and services, and carriers will need Program support at the front end of the process to make those payments. We recommend that the Commission incorporate reasonable milestones throughout the removal and replacement process so that carriers can demonstrate that their projects are moving forward and receive the additional funding they need upon demonstration that they have satisfied relevant milestones. This approach is consistent with the Secure Networks Act, which specifically notes that it shall not “be construed to prohibit the Commission from making a reimbursement under the Program . . . before the provider incurs the cost of the permanent removal, replacement, and disposal” for which it has applied for reimbursement,¹⁶ directs the Commission to collect “initial

¹⁵ *Public Notice* at 3.

¹⁶ Secure Networks Act § 4(h).

reimbursement cost estimate[s] at the time of application” (with “updated cost estimate[s]” as needed),¹⁷ and already requires periodic status updates from carriers to the Commission.¹⁸

The *Public Notice* also seeks comment on its interpretation of the Secure Networks Act as requiring an “express appropriation from Congress” and separation from any Universal Service Fund programs.¹⁹ CCA agrees with the Commission’s reading of the Secure Networks Act—funding for the Program must come from Congress, not from existing USF programs and in particular should not draw from vital high cost support. The Secure Networks Act directs the Commission to implement the reimbursement Program, with removal and replacement deadlines determined based on “the date on which the Commission distributes reimbursement funds to the recipient.”²⁰ We encourage the Commission to seek the necessary appropriation so that it can distribute funds quickly once they are available. Until that appropriation is available, we support the Commission as it takes its own steps forward to complete the rulemaking required by the Secure Networks Act and to ensure the success of the Program.²¹

II. REPLACEMENT PROCEDURES SHOULD ESTABLISH A REASONABLE GLIDE PATH THAT PRESERVES CONNECTIVITY FOR CONSUMERS

Reimbursing carriers for their expenses is only one aspect of ensuring the Program’s success, of course. The Secure Networks Act requires providers receiving funds to remove, replace, and dispose of covered equipment and services, and the Commission’s implementation of those sections of the statute must accommodate the complexity that process will entail.

¹⁷ *Id.* § 4(d)(2)(B).

¹⁸ *See id.* § 4(d)(8).

¹⁹ *Public Notice* at 3.

²⁰ Secure Networks Act § 4(d)(6)(A).

²¹ *See* Secure Networks Act § 4(g).

As the Commission implements the timeline of this program, it should be mindful of two current realities. First, we are in the middle of the biggest public health crisis of our lifetimes. Wireless carriers have been stepping up to the challenge by preserving and expanding connectivity, while trying to protect their employees, even as individuals and businesses across the country are facing substantial levels of unemployment and economic difficulty. Wireless carriers, including those with covered equipment, are working tirelessly to support their consumers, and understandably this pandemic is drawing significant resources that might otherwise be devoted to other key priorities. The second reality is that the Secure Networks Act is not yet funded. While CCA remains hopeful that Congress will appropriate funding to implement the statute, that funding has not yet materialized. In the face of the pandemic and the lack of appropriation, combined with the complex realities of transitioning network equipment while maintaining connectivity, the Commission should proceed with a reasonable perspective on expected timeline.

The Commission notes that the Secure Networks Act generally requires program recipients to complete their work within one year after the distribution of funds, but specifically authorizes the Commission to extend that baseline deadline to provide the necessary additional time.²² As described above, there are many stages to the process of transitioning network equipment, many of which will take significant time and are outside the control of carriers. For example, vendors likely will not be able to deliver equipment immediately after carriers place orders, and where carriers need to obtain additional space from third-party tower owners or permits from local authorities, carriers have limited ability to control those outside parties' review and approval processes. CCA members already have encountered vendors with 2-4-

²² *Public Notice* at 3.

month backlogs for equipment to test for future use. Equipment delivery timeframes may also extend as a consequence of the ongoing health crisis. CCA urges the Commission to implement the Program in a way that allows carriers that can demonstrate they are making progress and meeting milestones to get the time they need to do this important job while preserving connectivity for their customers.²³

The Commission specifically asks whether the Secure Networks Act permits it to grant both “general and individual extensions.”²⁴ CCA believes that it does. Section 4(d)(6)(C)(ii), which applies to individual extensions, expressly permits the Commission to grant individual extensions either of the initial one-year deadline “described in subparagraph (A)” or, “if the Commission has granted” a general extension “under subparagraph (B),” the deadline “as so extended.”²⁵ The Commission also asks whether it can “grant multiple extensions to an individual recipient if the circumstances warrant such action.”²⁶ Again, the answer is yes. While the statute limits the duration of particular extensions to “not more than 6 months,”²⁷ there is nothing in the text that suggests the Commission can grant individual recipients only a single extension where needed. A crabbed interpretation of the statute, by contrast, would seriously undermine the ability of some carriers to comply with deadlines, through no fault of their own, which could lead to service outages and other connectivity issues.

²³ The House Report accompanying H.R. 4998 suggests Congress anticipated that multiple extensions would be allowed by referring to plural “extensions.” *See* H.R. Rep. No. 116-352, at 14 (2019) (stating that “[t]he Commission may grant . . . individual extensions of an applicant’s deadline for not more than six months . . .”).

²⁴ *Public Notice* at 3.

²⁵ Secure Networks Act § 4(d)(6)(C)(ii).

²⁶ *Public Notice* at 3.

²⁷ Secure Networks Act § 4(d)(6)(C)(ii).

The Secure Networks Act requires the Commission to “develop a list of suggested replacements” for equipment, software, and services (or categories of the same) that is “technology neutral.”²⁸ The Public Notice seeks comment on how it should develop and maintain the list.²⁹ CCA supports an efficient design for this list so that it is functional for providers to use and not unduly burdensome for the Commission to update. To that end, CCA recommends that the Commission approve trusted vendors, rather than approve specific pieces of equipment. Equipment regularly evolves, and updating the list to reflect all new versions of equipment or services would be time-consuming and inefficient. Approval of a trusted vendor could presumptively extend to all of that vendor’s relevant equipment and services, with the Commission reserving the option of carving out, if necessary, problematic equipment or services from that vendor. The Public Notice asks whether Commission should include “suppliers of virtual network equipment and services.”³⁰ Virtual network equipment and services, including Open RAN and Virtual RAN, warrant further exploration, and in any event CCA encourages the Commission to implement this process on a technology-neutral basis. The determining factor should be whether the options offered by vendors can be demonstrated to work, not what technology they use.

The Secure Networks Act directs the Commission to issue regulations for “the disposal by a recipient of a reimbursement under the Program of covered communications equipment or services” that are “removed from the network of the recipient” to prevent their use in the networks of other providers.³¹ As the Commission considers how to implement that

²⁸ *Id.* § 4(d)(1)(A)-(B).

²⁹ *Public Notice* at 4.

³⁰ *Id.*

³¹ Secure Networks Act § 4(d)(7).

requirement, CCA again encourages it to take a flexible approach rather than artificially constrain providers' disposal options. For example, carriers should be permitted to satisfy the Commission's requirements by documenting their transfer of removed equipment to third parties tasked with destruction or other disposal of the equipment. It will be more efficient and realistic for the Commission to issue parameters to which disposal mechanisms must conform than for the Commission to attempt to prescribe *ex ante* precisely how that process should work for a wide variety of communications providers

* * *

CCA was pleased to see Congress's broad, holistic approach to the challenge of securing America's communications networks, and we look forward to continuing to work with the Commission as it implements Congress's directives and establishes the reimbursement Program.

Respectfully submitted,

/s/ Alexi Maltas

Alexi Maltas, SVP & General Counsel
Alexandra Mays, Policy Counsel
Competitive Carriers Association
601 New Jersey Ave. NW
Suite 820
Washington, DC 20001
(202) 747-0711

May 20, 2020